SETIT 2005
3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications
March 27-31, 2005 – TUNISIA

Security In Telemedicine: Issues In Watermarking Medical Images

Jasni Zain and Malcolm Clarke

Department of Information Systems and Computing, Brunel University, Uxbridge UB8 3PH, United Kingdom

Jasni.Zain@brunel.ac.uk
Malcolm.Clarke@brunel.ac.uk

Abstract: This paper opens a discussion about securing telemedicine by looking at attacks to the security by viewing the function of the computer system as provision of information. Categories of attacks are discussed and an overview of watermarking is introduced as one of the security tool, using the medical image as the channel for watermarking. The main objectives for medical image watermarking are that the watermarks are imperceptible and act as a mean of authentication and integrity control. The issues in watermarking medical images raised here are complete authentication Vs content authentication, reversible watermarking Vs permanent/irreversible watermarking and the practical issue of compression.
Key words: Security, Telemedicine, Watermarking

1. Introduction

One of the major concerns through out the world today is to make high quality health care available to all. Traditionally, part of the difficulty in achieving equitable access to health care has been that the provider and the recipient must be physically present in the same place. Recent advances in information and communication technologies have increased the number of ways health care can be delivered to reduce these difficulty.

Telemedicine, the area where medicine and information and telecommunications technology meet, is probably the part of this revolution that could have the greatest impact on health care delivery. The prefix 'tele' derives from the Greek 'at a distance', and therefore, more simply telemedicine is medicine at a distance. The information infrastructure of modern health care is based on digital information management. While the recent advances in information and communication technologies provide new means to access, handle and move medical information, they also compromise their security due to their ease of manipulation and replication. All patients records, electronic or not, linked to medical secrecy, must be confidential. The digital handling of EPR (Electronic Patient Record) on network requires a systematic content validation that is aimed at quality control: actuality (precise interest of the information at a given instant) and reliability (authentication of the origin and integrity).

2. Security attacks

Attacks on security are best characterized by viewing the function of the computer system as provision of information. In general, normal communication is represented as a flow of information from a source to a destination

There are four categories of attacks:

- Interruption: An attack on availability. Information is destroyed or becomes unavailable or unusable.
- Interception: An attack on confidentiality. An unauthorized party gains access to information.
- Modification: An attack on integrity. An unauthorized party not only gains access to, but also tampers with information.
- Fabrication: An attack on authenticity. An unauthorized party inserts counterfeit objects into the system.

The attacks can be divided into two categories, according to the nature of the attacks:

- Active Attacks: These attacks involve modification of data stream or the creation of a false stream and can be subdivided into four categories:
    1. Masquerade: One entity pretends to be a different entity.

2. Replay: One passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
3. Modification of messages: Some portion of a legitimate message is altered, or message are delayed or recorded to produce an unauthorized effect.
4. Denial of service: One prevents or inhibits the normal use or management of communications facilities.

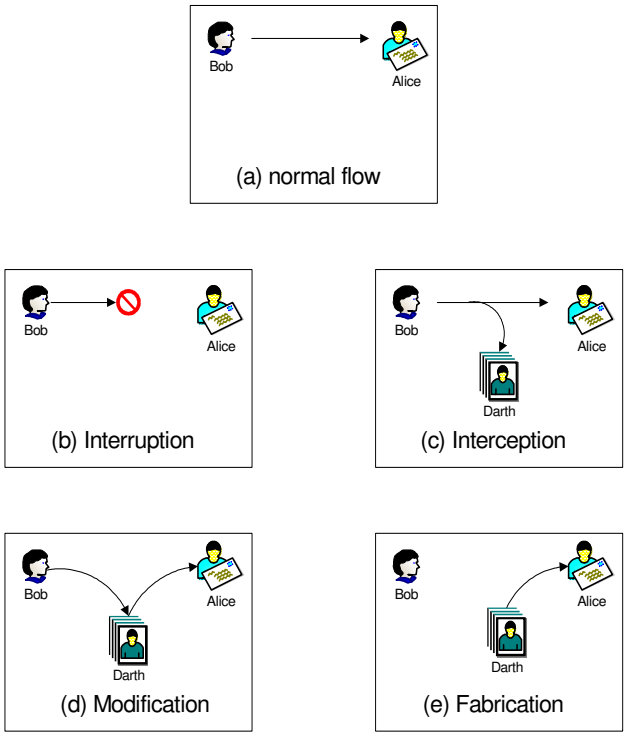

Figure 1 *Security Attacks*

- Passive Attacks: These attacks involve eavesdropping on, or monitoring of, transmission and can be subdivided into two categories:
- Release of message contents: An unauthorised party obtains information that is being transmitted.
- Traffic analysis: An unauthorised party obtains information useful in guessing the nature of communication by observing the pattern of masked message transmissions.

The next section will introduce watermarking and steganography as a security tool to deal with modification and fabrication.

3. Watermarking and Steganography

Watermarking, that is the technique of placing and transmitting small amount of data imperceptibly in host or cover data, has many applications including broadcast monitoring, owner identification, proof of ownership and content authentication. However, steganography or data hiding has been studied long before and the use of paper watermarks for copy protection can be traced back until the thirteenth century (Murray 1996). The earliest forms of information hiding can actually be considered to be highly crude forms of private-key cryptography; the "key" in this case being the knowledge of the method being employed (security through obscurity). Steganography books are filled with examples of such methods used throughout history. Greek messengers had messages tattooed into their shave head, concealing the message when their hair finally grew back. Wax tables were scraped down to bare wood where a message was scratched. Once the tables were re-waxed, the hidden message was secure (Petitcolas, Fabien A. P. 2000). Over time these primitive cryptographic techniques improved, increasing speed, capacity and security of the transmitted message. Today, crypto-graphical techniques have reached a level of sophistication such that properly encrypted communications can be assumed secure well beyond the useful life of the information transmitted. In fact, it is projected that the most powerful algorithms using multi kilobit key lengths could not be comprised through brute force, even if all the computing power worldwide for the next 20 years was focused on the attack. Of course the possibility exists that vulnerabilities could be found, or computing power breakthroughs could occur, but for most users in most applications, current cryptographic techniques are generally sufficient.

Why then pursue the field of information hiding? Several good reasons exist, the first being that "security through obscurity" is not necessarily a bad thing, provided that it is not the only security mechanism employed. Steganography for instance allows us to hide encrypted messages in mediums less likely to attract attention. A garble of random characters being transmitted between two users may tip off a watchful third party that sensitive information is being transmitted; whereas baby pictures with some additional noise present may not. The underlying information in the pictures is still encrypted, but attracts far less attention being distributed in the picture then it would otherwise.

Nowadays, there exist watermarking methods for virtually every kind of digital media: text documents (Su & al. 1998, Brassil & al. 1999), images (Tsai & al. 2004, Zhang & al. 2003, Paquet & al. 2003), video (Sun & al. 2003, Okada & al. 2002), audio (Li & al. 2003, Yan & al. 2004), even for 3D polygonal models (Kwon & al. 2003, Benedens & al. 2000), maps (Barni & al. 2001) and computer programs (Monden & al. 2000). Interestingly, watermarking technology is not limited to digital media, but also applicable to for

example chemical data like protein structure (Eggers & al. 2001).

4. Medical image watermarking

Security of medical images, derived from strict ethics and legislative rules, gives rights to the patient and duties to the health professionals. This imposes three mandatory characteristics: confidentiality, reliability and availability:

- Confidentiality means that only the entitled persons have access to the images;
- Reliability which has two aspects; Integrity: the image has not been modified by non-authorized person, and authentication: a proof that the image belongs indeed to the correct patient and is issued from the correct source;
- Availability is the ability of an image to be used by the entitled persons in the normal conditions of access and exercise.

Security risks of medical images can vary from random errors occurring during transmission to lost or overwritten segments in the network during exchanges in the intra- and inter-hospital networks. One must also guarantee that the header of the image file always matches that of the image data. In addition to these unintentional modifications one can envision various malicious manipulations to replace or modify parts of the image, called tampering. The usual characteristics of watermarking are invisibility of the mark, survives common distortions, carries many bits of information, secrecy to unauthorized persons, and requires little computation to insert or detect (Miller et al. 1999). These demands also exist in the medical domain but additional constraints are added. Three main objectives are foreseen in the medical domain (Coatrieux & al. 2000, Mintzer & al. 1997):

4.1 Imperceptible / Reversible Watermarking

Medical tradition is very strict with the quality of biomedical images. Thus the watermarking method must be reversible, in that the original pixel values must be exactly recovered (Macq & al. 1999). This limits significantly the capacity and the number of possible methods. An alternative way is to define regions of interest, to be left intact, and leave us with regions of insertion where watermark could be inserted and does not interfere or disturb the radiologist.

4.2. Integrity Control

The “trustworthy camera” concept applies also to medical images, especially in the context of legal aspects and insurance claims. Friedman has used this concept in his work (Friedman 1993). By embedding an encryption chip in the camera, the camera endorses its captured pictures and generates content-dependant digital signatures. There is thus a need to prove that, the images on which the diagnoses and any insurance claims are based have preserved their integrity.

4.3. Authentication

A critical requirement in patient records is to authenticate the different parts of the electronic patient record, in particular the images. More often an attached file or a header, which carries all the needed information, identifies an image. However, keeping the meta-data of the image in a separate header file is prone to forgeries or clumsy practices. An alternative would be to embed all such information into the image data itself.

The studies that are specifically directed to watermarking of medical images are few. (Anand & al. 1998) propose to embed an encrypted version of the Electronic Patient Record (EPR) in the least significant bit (LSB) plane of the image. While this scheme may seem to affect minimally the diagnostic content the ease with which the LSB plane can be manipulated is well known. (Miaou & al. 2000) similarly propose a LSB technique where the host image authenticates the transmission origin with an embedded message composed of various patient data (e.g ECG record), the diagnosis report and the doctor’s seal. (Macq & al. 1999), propose a trusted header scheme by embedding the hash of the file header of medical standard image in the image raw data. (Coatrieux & al. 2001) propose Region of Interest (ROI) to preserve the diagnostic zone and Region of Non Interest (RONI) whose integrity needs not be preserved and serves as the watermark carrier. Trichili & al. (2002) proposes an image virtual border as the watermarking area. Patient’s data is then embedded in the LSBs of the border. Guo & al. (2003) present a scheme where the digital signature of the whole image and patient information is embedded. Cao & al. (2003) extend their work on digital envelope (DE) and embed their DE by making a random walk sequence and replace LSB of each selected pixel.

Previous studies do not address the issues of normal image processing such as compression. Since most of previous studies use LSB as the watermarking domain, which is known as a fragile technique, allowing compression will almost certainly will destroy the watermark. The next section will highlights some issues relevant to watermarking medical images.

5. Issues in watermarking medical images

A few issues need to be clarified before choosing tools and techniques for this research. The first issue to consider is either a complete authentication or content authentication will be used. Complete authentication refers to techniques that consider the whole piece of image and do not allow any manipulations or transformation (Wu & al. 1998, Yeung & al. 1997). Many existing message authentication techniques can be applied directly. For

instance, digital signatures can be placed in the LSB of uncompressed data, or the header of compressed data. Manipulations will be detected if the hash value of the altered message bits does not match the information in the digital signature. In practice, fragile watermarks or traditional digital signatures may be used for complete authentication. Content authentication refers to a different objective that is unique to multimedia data. The meaning of multimedia data is based on their content instead of the bit streams. In some applications, manipulations on the bit streams without changing the meaning of content are considered as acceptable. Compression is an example. Digital Imaging and Communication in Medicine (DICOM) standard has included JPEG (lossy and lossless), JPEG-LS and RLE (known as TIFF) compressions in their standard. JPEG2000 has also been considered in the report (National Electrical Manufacturers Association (NEMA) 2002).

The second issue is either the watermarks are reversible or permanent. As the point of strict specification for medical images has been raised by several researchers (Macq, Dewey 1999, Giakoumaki, Pavlopoulos & Koutsouris 2003, Yang, Bao 2003) the need for watermarks to be reversible in the case of medical imaging is suggested. On the other hand, one can also argue that if distortion is allowed through compression, it should also be allowed for watermarks as long as they do not interfere with the diagnosis.

The third issue is if we decide to have watermarks for content authentication, compression should be distinguished from other manipulations. Previous watermarks are either too fragile for compression or too flexible to detect malicious manipulations. The performance of an authenticator should be simultaneously evaluated by two parameters: the probability of false alarm and the probability of missing manipulations. Fragile watermarks, which have low probability of miss, usually fail to survive compressions such that their probability of false alarm is very high. Previous researchers have attempted to modify the fragile watermark to make it robust with compression (Zhu, Swanson & Tewfik 1996, Wolfgang, Delp 1996). However, such modifications failed to distinguish compression and tampering. On the other hand, robust watermarks are robust to most manipulations and are usually too robust to detect malicious manipulations.

Regardless of security issues, watermarking capacity is determined by invisibility and robustness requirements. A conceptual description is shown in Figure 2. There are three dimensions in this figure. If one parameter is determined, the other two parameters are inverse-proportional. For instance, a specific application may determine how many message bits are needed, copyright protection may need to embed about 10 bytes and authentication may need from 100-1000 bits for a 265 X 256 image. After the embedded amount is decided, there always exists a trade-off between visual quality and robustness. Robustness refers to the extraction of embedded bits with an error probability equal to or approaching zero. Visual quality represents the quality of watermarked image. In general, if we want to make our message bits more robust against attack, then a longer codeword will be necessary to provide better error resistance. However, visual quality degradation can be expected.

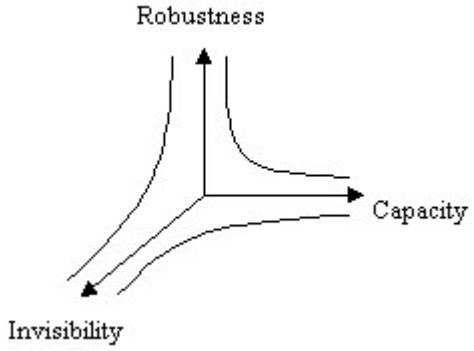

Figure 2 *Watermarking properties*

Conclusion

Watermarking is a potential technique to address the issue of reliability of medical images namely for verifying integrity and authentication. Since compression is included in standards such as DICOM, researchers in the area of medical watermarking need to strategize their research to make sense with common practice.

References

Anand, D. & Niranjan, U. 1998, "Watermarking Medical Images with Patient Information", *IEEE/EMBS Conference*, pp. 703-706.

Barni, M., Bartolini, F., Cappellini, V., Piva, A. & Salucco, F. 2001, "Text-based geometric normalization for robust watermarking of digital maps", *IEEE International Conference on Image Processing (ICIP) 2001, Oct 7-10 2001*Institute of Electrical and Electronics Engineers Computer Society, Thessaloniki, pp. 1082-1085.

Benedens, O., Busch, C. 2000, "Towards blind detection of robust watermarks in polygonal models", *Computer Graphics Forum,* vol. 19, no. 3, pp. 199-208.

Brassil, J.T., Low, S. & Maxemchuk, N.F. 1999, "Copyright protection for the electronic distribution of text documents", *Proceedings of the IEEE,* vol. 87, no. 7, pp. 1181-1196.

Cao, F., Huang, H.K. & Zhou, X.Q. 2003, “Medical image security in a HIPAA mandated PACS environment,” *Comput. Med.Imaging Graphics*, vol. 27, pp. 185-196.

Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y. & Collorec, R. 2000, "Relevance of Watermarking in Medical Imaging", *2000 IEEE EMBS Conf. On Information Technology Applications in Biomedicine*, pp. 250-255.

Coatrieux, G., Sankur, B. & Maitre, H. 2001, "Strict

Integrity Control of Biomedical Images", *SPIE Conf. 4314: Security and Watermarking of Multimedia Contents III*.

Eggers, J.J., Ihlenfeldt, W.. & Girod, B. 2001, "Digital watermarking of chemical structure sets", *Proceedings of the 4th Information Hiding Workshop '01*.

Friedman, G.L. 1993, "The Trustworthy Digital Camera: Restoring Credibility to the Photographic image", *IEEE Transactions on Consumer Electronics,* vol. 39, no. 4, pp. 905-910.

Giakoumaki, A., Pavlopoulos, S. & Koutsouris, D. 2003, "A medical image watermarking scheme based on wavelet transform",*Proceedings of 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 856-859.

Guo, X. & Zhuang, T. 2003, " A lossless watermarking scheme for enhancing security of medical data in PACS," *Proceedings of Medical Imaging 2003: PACS and Integrated Medical Information Systems: Design and Evaluation*, pp. 350-359.

Kwon, K., Kwon, S., Lee, S., Kim, T. & Lee, K. 2003, "Watermarking for 3D polygonal meshes using normal vector distributions of each patch", *Proceedings: 2003 International Conference on Image Processing, ICIP-2003,* pp. 499-502.

Li, W., Xue, X. 2003, "An audio watermarking technique that is robust against random cropping", *Computer Music Journal,* vol. 27, no. 4, pp. 58-68.

Macq, B. & Dewey, F. 1999, "Trusted Headers for Medical Images", *DFG VIIII-DII Watermarking Workshop*.

Miaou, S.-., Hsu, C.-., Tsai, Y.-. & Chao, H.-. 2000, "A secure data hiding technique with heterogeneous data-combining capability for electronic patient records", *22nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society,* pp. 280-283.

Miller, M.L., Cox, I.J., Linnartz, J.M.G. & Kalker, T. 1999, "A Review of Watermarking Principles and Practices" in *Digital Signal Processing for Multimedia Syatems*, eds. K.K. parhi & T. Nishitani, Marcel Dekker Inc., New York.

Mintzer, F., Braudaway, G.W. & Yeung, M.M. 1997, "Effective and ineffective digital watermarks", *Proceedings of the 1997 International Conference on Image Processing. Part 3 (of 3)*, pp. 9-12.

Monden, A., Iida, H., Matsumoto, K., Inoue, K. & Torii, K. 2000, "Practical method for watermarking Java programs", *2000 IEEE 24th Annual International Computer Software and Applications Conference (COMPSAC 2000),* pp. 191-197.

Murray, T.D. 1996, *The Wizard of Watermarks* [Homepage of Virginia Tech.], [Online]. Available: http://ebbs.english.vt.edu/gravell/wizard/wizard.html [2004, June 30].

National Electrical Manufacturers Association (NEMA) 2002, 28 March 2002-last update*, DICOM Strategic Document*. Available: http://www.amicas.com/pacsed/DICOM%20Strategy_2002-03-28.doc [2004, 6 July 2004].

Okada, H., Shiitev, A., Song, H., Fujita, G., Onoye, T. & Shirakawa, I. 2002, "Error detection by digital watermaking for MPEG-4 video coding", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,* vol. E85-A, no. 6, pp. 1281-1288.

Paquet, A.H., Ward, R.K. & Pitas, I. 2003, "Wavelet packets-based digital watermarking for image verification and authentication*1", *Signal Processing,* vol. 83, no. 10, pp. 2117-2132.

Petitcolas, Fabien A. P. 2000, "Introduction to Information Hiding" in *Information Hiding Techniques for Steganography and Digital Watermarking*, eds. S. Katzenbeisser & Petitcolas, Fabien A. P., Artech House, Norwood, MA.

Su, J.K., Hartung, F. & Girod, B. 1998, "Digital watermarking of text, image, and video documents", *Computers & Graphics,* vol. 22, no. 6, pp. 687-695.

Sun, S. & Chang, P. 2003, "Video watermarking synchronization based on profile statistics", *Proceedings: 37th Annual 2003 International Carnahan Conference on Security Technology,* pp. 410-413.

Trichili, H., Bouhlel, M., Derbel, N., & Kamoun, L. 2002, "A new medical image watermarking scheme for a better telediagnosis," in 2002 IEEE International Conference on Systems, Man and Cybernetics, pp. 557-560.

Tsai, P., Hu, Y. & Chang, C. 2004, "A color image watermarking scheme based on color quantization", *Signal Processing,* vol. 84, no. 1, pp. 95-106.

Wolfgang, R.B. & Delp, E.J. 1996, "A watermark for digital images*", International Conference on Image Processing* , pp. 219-222.

Wu, M. & Liu, B. 1998, "Watermarking for image authentication", *Proceedings of the 1998 International Conference on Image Processing, ICIP. Part 2 (of 3),* pp. 437-441.

Yan, F., Ji, B., Zhang, D. & Fang, H. 2004, "Robust quadri-phase audio watermarking", *Acoustical Science and Technology,* vol. 25, no. 1, pp. 106-108.

Yang, Y. & Bao, F. 2003, "An invertible watermarking scheme for authentication of electronic clinical brain atlas", *2003 IEEE International Conference on*

Accoustics, Speech, and Signal Processing, pp. 533-536.

Yeung, M.M. & Mintzer, F. 1997, "An invisible watermarking technique for image verification", *International Conference on Image Processing*, pp. 680-683.

Zhang, X., Feng, J. & Lo, K. 2003, "Image watermarking using tree-based spatial-frequency feature of wavelet transform", *Journal of Visual Communication and Image Representation,* vol. 14, no. 4, pp. 474-491.

Zhu, B., Swanson, M.D. & Tewfik, A.H. 1996, "Transparent robust authentication and distortion measurement technique for images*", Digital Signal Processing Workshop*, pp. 45-48.